(19) RU (11) 2 124 814 (13) C1

(51) Int. Cl.[6] H 04 L 9/00

RUSSIAN AGENCY
FOR PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: 97121649/09, 24.12.1997

(46) Date of publication: 10.01.1999

(98) Mail address:
197022 Sankt-Peterburg, ul.Kantemirovskaja 10, STsPS "SPEKTR"

(71) Applicant:
Moldovjan Nikolaj Andreevich,
Moldovjan Aleksandr Andreevich,
Gosudarstvennoe unitarnoe predprijatie Spetsializirovannyj tsentr programmnykh sistem "SPEKTR"

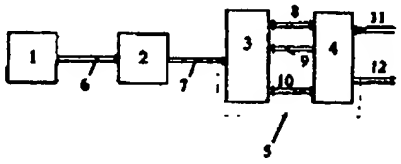
(72) Inventor. Moldovjan A.A., Moldovjan N.A., Moldovjanu P.A.

(73) Proprietor.
Moldovjan Nikolaj Andreevich,
Moldovjan Aleksandr Andreevich,
Gosudarstvennoe unitarnoe predprijatie Spetsializirovannyj tsentr programmnykh sistem "SPEKTR"

(54) METHOD FOR ENCODING OF DIGITAL DATA

(57) Abstract:

FIELD: communication, computer engineering, in particular, cryptography. SUBSTANCE: method involves generation of secret key, splitting data records into N blocks, and sequential conversion of blocks by running at least one conversion for i-th block, depending on value of j-th block, where j is not equal to i. In addition after generation of secret key method involves generation of encryption algorithm depending on value of secret key by running at least one conversion operation over i-th block Said conversion operation is designed as substitution EFFECT: increased resistance to known methods of cryptanalysis, including differential and linear cryptanalysis. 2 cl, 3 dwg



Фиг. 1.

RU 2124814 C1

RU 2124814 C1

The invention pertains to the field of electronic communication and computer technology and, more specifically, to the field of cryptographic methods and devices for encryption of information. The following terms are used in the group of features of the claimed method:

- a secret key is binary information known only to a lawful user,

- subkey – element of a secret key, represented as a group of subkeys,

- encryption is a process of conversion of information that depends on a secret key and converts the initial text to ciphertext, which represents a pseudorandom sequence of symbols, from which information cannot be obtained without knowledge of the secret key

- decoding is a process inverse to the encryption process, decoding ensures restoration of the information according to a cryptogram with knowledge of the secret key,

- a code represents a group of elementary steps of conversion of initial data, using a secret key. The code can be implemented in the form of a computer program or in the form of a separate device,

- cryptanalysis – method of calculating a secret key to obtain unsanctioned access to encrypted information or development of a method that ensures access to encrypted information without calculation of the secret key,

- cryptanalyst – a person who performs cryptanalysis, i.e., attacks the code,

- cryptographic integrity is a gauge of the reliability of protection of encrypted information and represents the labor required, measured in number of elementary operations necessary to restore the information according to a cryptogram, when the conversion algorithm is known, but without knowledge of the secret key. In the case of unidirectional conversions, cryptographic integrity is understood to mean the complexity of calculating the initial value of a block according to its output value.

- cyclic shift operations, which depend on the subblocks being converted or depend on a binary vector – these are operations of a cyclic shift by a number of bits assigned by the value of the subblock or by the value of a binary vector; a cyclic shift operation to the left (right) is denoted with the symbol "<<<" (">>>"), for example, the notation $B_1 < B_2$ denotes a cyclic shift operation to the left of subblock B_1 by a number of bits equal to the value of the binary vector B_2

- one-place operation – an operation performed on one operand (block of data or binary vector), the value of a subblock after performance of a certain given one-place operation depends only on its initial value, examples of one-place operations are cyclic shift operations,

- two-place operation – operation performed on two operands; the result of performance of a certain given two-place operation depends on the value of each operand, examples of two-place operations are addition, subtraction, multiplication operations, etc.,

- superposition of a subkey on a subblock – this is a procedure of performing a two-place operation (*) on a subblock (B) and subkey (Q) and assignment of the result of performance of

this operation to the subblock, which is analytically written in the form of the formula B < -B*Q, where "<-* is the sign of the assignment operation.

Methods are known for block encryption of data (see, for example, US Standard DES (National Bureau of Standards Data Encryption Standard Federal Information Processing Standards Publication 46, January 1977, see also S. Maftik, Mechanisms of Protection in Computer Networks – Moscow, Mir, 1993, pages 42-47). In this method, encryption of data blocks is performed by forming a secret key, breakdown of the data block being converted into two subblocks L and R and a sequential change in the latter by performing an operation of digit-by-digit summing modulo 2 on subblock L and with a binary vector, which is formed as an output value of a certain function F from the value of subblock R. After this, the blocks are transposed in positions. Function F in this method is accomplished by performing transposition and substitution operations, performed on subblock R. This method possesses high speed of conversions, when implemented in the form of specialized electronic circuits.

However, the known analog method uses a secret key of small size (56-bit), which makes it vulnerable to cryptanalysis based on key selection. The latter is associated with the high calculation capacity of modern computers in general use.

The method closest in technical essence to the one proposed for cryptographic conversion of L-bit input blocks of digital data to L-bit output blocks is a method implemented in the RC5 code, described in the paper of R. Rivest, The RC5 Encryption Algorithm/Fast Software Encryption, Second International Workshop Proceedings (Leuven, Belgium, December 14-16, 1994), Lecture Notes in Computer Science, Vol. 1008, Springer-Verlag, 1995, pages 86-96. The prior art method includes formation of a secret key in the form of a group of subkeys, breakdown of the input block of data into subblocks A and B and sequential conversion of the subblocks. The subblocks are converted by performing one-place and two-place operations on them. As two-place operations, modulo 2^n addition is used, where n = 8, 16, 32, 64, and modulo 2 digit-by-digit summing. As one-place operation, a cyclic shift to the left is used, in which the number of bits, by which the subblock being converted is shifted, depends on the value of the second subblock, which determines the dependence of the cyclic shift operation in the current conversion step of the subblock on the initial value of the input block of data. A two-place operation is performed on the subblock and subkey, and also on two subblocks. A characteristic of the prior art method is the use of cyclic shift operations that depend on the value of the input block.

The subblock, for example, subblock B, is converted by the following method. A digit-by-digit summing operation modulo 2 is performed on subblocks A and B and the value obtained after performance of this operation is assigned to subblock B. This is written in the form of the relation $B \leftarrow B \oplus V$, where the sign "< -" denotes the assignment operation and the sign "$\oplus$" denotes digit-by-digit summing Modulo 2. After this, a cyclic shift operation is performed on subblock B by a number of bits equal to the value of subblock A B < - B <<< A. A summing operation modulo 2^n is then performed on the subblock and one of the subkeys S, where n is the length of a subblock in bits B < - B+S mod 2^n. After this, block A is converted similarly. Several such steps of conversion of both subblocks are performed.

This method ensures high rate of encryption, when implemented in the form of a computer program. However, the prior art method has drawbacks, namely, during implementation for computers with a 32-bit microprocessor, it does not ensure high resistance of cryptographic transformation of data to differential and linear cryptanalysis (Kaliski B. S., Yin Y. L., On Differential and Linear Cryptanalysis of the RC5 Encryption Algorithm, Advances in Cryptology – CRYPTO '95 Proceedings, Springer-Verlag, 1995, pages 171-184). This drawback is associated with the fact that the effectiveness of using operations that depend on the data being converted, in order to complicate known methods of cryptanalysis, is reduced by the fact that the encryption algorithm is known to the cryptanalyst, which enables the latter to determine the statistical characteristics of the encryption procedure and to use them in performing cryptanalysis.

The task underlying the invention is to develop a method for encryption of blocks of digital data, in which encryption of the input data would be accomplished, so that determination of the statistical features of the encryption algorithm by a cryptanalyst would be significantly hampered, by virtue of which the resistance to known methods of cryptanalysis is increased, including differential and linear cryptanalysis.

This task is achieved in that, in the method for cryptographic conversion of blocks of digital data, consisting of formation of a secret key, breakdown of a data block into N>2 subblocks and sequential conversion of the subblocks by performance on the subblock of at least one conversion operation, which depends on the value of the input block, the new feature according to the invention is that, after formation of the secret key, an encryption algorithm is additionally formed as a function of the secret key.

By virtue of this solution, a significant complication in determining the statistical features of the encryption algorithm by cryptanalysis is ensured, by virtue of which increased resistance of the cryptographic conversion to known methods of cryptanalysis is ensured.

It is also new that one of the subblocks is additionally converted by accomplishing substitution operations on it, which depends on the input block and is performed according to secret substitution tables. By virtue of this solution, an additional increase in cryptographic integrity relative to known methods of cryptanalysis is ensured.

It is also new that the encryption algorithms are formed by formation of operations that depend on the input block.

By virtue of this solution, an additional increase in cryptographic integrity relative to known methods of cryptanalysis is ensured. It is also new that the encryption algorithm is formed by formation of substitution operations that depend on the input block and are accomplished according to secret substitution tables.

Owing to this solution, an additional increase in cryptographic integrity relative to known methods of cryptanalysis is ensured.

The essence of the claimed invention is explained in greater detail below by examples of its accomplishment, with reference to the appended drawings.

Figure 1 shows a generalized diagram of a cryptographic device for encryption of blocks of digital data according to the claimed method

Figure 2 shows an encryption scheme corresponding to example 1

Figure 3 shows an encryption scheme corresponding to example 3

The claimed method can be implemented with the computer of a calculation device, represented by the block diagram in Figure 1, where

block 1 is the input device for the secret key,

block 2 is the unit for formation of the machine code of the encryption program (cipher setup unit),

block 3 is the memory unit of the encryption device,

block 4 is the operating unit of the encryption device, containing three, four or more registers,

block 5 is the encryption device,

6 is a transmission line of information signals of the secret key of the user,

7 is a transmission line of information signals on the formed machine code of the encryption program and secret key,

8 is a transmission line of information signals of the subkeys and transmission of information signals of the input data and information signals of the subblocks being converted,

9 is the address line,

10 is the transmission line of information signals of the machine code of the encryption program,

11 is the input line of the input data,

12 is the output line of the ciphertext.

Formation of the secret code can be accomplished directly by introducing it to the ciphering system or the working memory of the computer, for example, from a removable information carrier. The input data block is broken down into subblocks, for example, by representation of the subblock in the form of a group of subblocks written according to fixed addresses in the memory unit 3.

Using block 1, a secret code is introduced, the information signal of which is fed along line 6 to the input of block 2. In block 2, the encryption algorithm is formed as a function of the secret key, i.e., a machine code of the encryption program is generated under the control of the secret key. Formation of the encryption algorithm is accomplished so that any modification of the encryption algorithm includes breakdown of the block of digital data into subblocks and sequential conversion of the subblocks by performing a two-place operation on the subblock and subkey and performance on the subblock of a conversion operation that depends on the input blocks.

The information signal of the secret key and the information signal of the machine code of the encryption program are sent along line 7 to the memory block 3. After this, the encryption device 5 contains in the memory a secret key and a machine code that implements the formed encryption algorithm and is ready to perform the encryption operations. This initialized state of the device is retained throughout operation of a lawful user. The input block of digital data is introduced along line 11 to the operating block 4, and then along line 8 to the memory block 3. The ciphertext block is read out from line 12. The codes of the machine commands to perform the conversion procedures are transmitted along line 10 to the operating block 4. On completion of encryption of the data, the user disengages the encryption device, which leads to automatic

erasure of the secret key and the formed machine code of the encryption algorithm from the memory region of block 2 and block 3, since power supply of all the blocks of the encryption device is cut off. Thus, the specific modification of the encryption algorithm, and also the secret key, are inaccessible to a potential cryptanalyst, who only knows the algorithm of formation of the encryption algorithm. This significantly hampers determination of the statistical characteristics of the specific modification of the encryption algorithm. At a number of potentially performable modifications equal to or greater than 10^{20}, the claimed method of encryption ensures high resistance to all known cryptanalysis methods.

Formation of the encryption algorithm can be accomplished as follows. Initially, based on one of the known algorithmic languages, a program template is compiled. Locations in which the possibility of writing any of a certain set of operations (for example, two-place operations or cyclic shift operations that depend on the input block) is provided, are reserved in the program template. All the reserved sites (under conversion operations) are numbered. In sequence, beginning from the first, conversion operations are formed for all reserved sites as a function of the value of the element of an additional pseudorandom sequence, having a number that coincides with the number of the operation being set up. Generation of the pseudorandom sequence of necessary length is accomplished as a function of the secret key, for example, using pseudorandom number generators described in the paper of Brikell E. F., Odlishko Z. M., Cryptanalysis: Review of Recent Results, TIIER, 1988, Vol. 76, No. 5, pages 87-89.

Formation of conversion operations is accomplished, for example, as follows. The two-place operation, used to superimpose the subkey on the subblock, is established as an operation of digit-by-digit summing modulo 2 ($\oplus$), if $d_j \bmod 3 = 0$, where d_j is the value of the corresponding element of the additional pseudorandom sequence, or as an operation of summing Modulo 2^{32} (Φ), of $d_j \bmod 3 = 1$, or as an operation of subtraction Modulo 2^{32} (-), if $d_j \bmod 3 = 2$. In the procedures of setting up the decoding algorithm, the operations that are inverse relative to the corresponding operations set up in the encryption algorithm are set up. For this purpose, the binary operation and the decoding algorithm are established as an operation of digit-by-digit summing Modulo 2 ($\oplus$), if $d_j \bmod 3 = 0$, or as an subtraction operation modulo 2^{32} (-), if $d_j \bmod 3 = 1$, or as a modulo 2^{32} summing operation (+), if $d_j \bmod 3 = 2$.

After this, as in the encryption program written in the algorithmic language (for example, in SI language or Pascal), the conversion operations are established in all the reserved sites, the machine code is generated corresponding to the encryption program, using, for example, a translator that converts the program compiled in algorithmic language to a sequence of machine

commands. The secret key and machine code of the encryption program are written in the working memory of the computer (or a specialized digital device) and are found there permanently throughout operation of a given user, performing conversion of blocks of data arriving for encryption. The complexity of the procedure of formation of the encryption key and generation of the machine code of the encryption program does not affect the encryption speed, since this procedure is performed once during identification of the user, according to a password, at the moment of engagement of the digital device or call-up of the encryption program.

An additional increase in cryptographic integrity of encryption is achieved during assignment of formation of the conversion operations, depending on the data being converted. For example, for positions reserved under a one-place operation on one of the 32-bit subblocks being converted – subblock B_1, formation of one of the following operations can be assigned: (1) substitution operations (^1S_v) on 8 younger binary bits (with numbers from 1 to 8) of a subblock, performed according to a v-th substitution table, the number of which is chosen as a function of subblock Bj, where $i \neq j$, (2) by a similar substitution operation of (^2S_v) on binary bits of the subblock with numbers from 9 to 16 inclusive, (3) cyclic shift operations to the left ($<<<_1V$) of the contents of the subblock by a number of bits equal to $V = B_I \bmod 32$, where $I \neq j$, (4) cyclic shift operations to the left ($<<<_2V$) of the contents of the younger 16 binary bits of the subblock by a number of bits equal to $V = Bj \bmod 16$, where $i \neq j$, (5) cyclic shift operations to the left ($<<<_3V$) of the contents of the younger 8 binary bits of the subblock by a number of bits equal to the value $V = B_I \bmod 8$, where $i \neq j$, (6) cyclic shift operations to the left ($<<<_4V$) of the contents of the binary bits from 9 to 16 inclusive, of the subblock by a number of bits equal to the value $V = Bj \bmod 8$, where //illegible//.

After this, as in the encryption program written in algorithmic language (for example, in SI or Pascal language), the conversion operations are established in all reserved sites, a machine code is generated corresponding to the encryption program, using, for example, a translator that converts the program compiled in algorithmic language to a sequence of machine commands. The secret code and machine code of the encryption program are written in the working memory of the computer (or specialized encryption device) and are found there constantly throughout the operating time of the given user, performing conversion of blocks of digital data arriving for encryption.

The complexity of the procedures for formation of the encryption key and generation of machine code of the encryption program does not affect the rate of encryption, since this procedure is performed once during identification of the user according to a secret key at the

moment of engagement of the encryption device or call-up of the encryption program. In modern computers, the procedure of formation of an encryption algorithm in the form of a machine code of an encryption program can be easily automated and implemented in the form of an initialization program of the encryption module. The time required to perform the initialization program is from 0.03 to 0.5 sec, depending on the specific variant of the claimed method, which is acceptable for most applications of information protection systems.

The decoding program of the blocks of the cryptogram is formed similarly. The encryption and decoding program corresponding to it form a single cryptographic program. For machine coding, the cryptographic program is written in the working memory of the computer, which, under its control, performs the encryption and decoding procedure of the blocks. The encryption procedure and encryption key are formed as a function of the secret key (password) of the user, i.e., are unique, which ensures high complexity of cryptanalysis.

An important type of operation that depends on the data being converted is represented by substitution operations accomplished according to tables, selected as a function of the input block. Let the substitution operation be performed on subblocks of digital data with a length of k-bit, where k is an integer. During assignment of the substitution operation that converts the k-bit input subblock to a k-bit output subblock, the use of a table containing two lines of numbers is then required

0 1 2 ... N-1

a_0 a_1 a_2 ... a_{N-1},

where $N = 2^k$.

All possible values of the k-bit block are present in this table in the lower line exactly once, but in an arbitrary sequence. The sequence of positioning of the numbers in the lower line determines the specific variant of the substitution table and, consequently, the specific variant of the substitution operation performed using this table. Performing of a substitution operation is accomplished as follows. The number equal to the value of the input block is selected in the upper line. The value located beneath this number in the lower line is taken as output block. Thus, the substitution table can be placed in the working memory of the computer as a sequential writing of k-bit computer words, placed in cells with addresses W_0, W_1, W_2, ... W_{N-1}. In this case, the value of the input block b serves to calculate the address $W_0 + b$ of the word that is taken as output block. This method of presentation of the substitution table requires the use of a memory volume equal to kN-bit.

We select the number of substitution tables equal to 2^L (the volume of required memory here is $2^L kN$ bit) and place the substitution tables directly next to each other. As address of the table with number V, we take the value of the address W_0 of its first k-bit word. Let the address of the table with number 0 be s. In this case, the address of the substitution table, with an arbitrary number V, equals s + VN. If the number of the current substitution table V and the current input subblock are assigned for performance of the substitution operation, it is performed by replacement of the current input block by a k-bit word, situated according to the address s + VN + b, where b is the value of the subblock, on which the current substitution operation is performed. Using this relation, it is easy to assign selection of the substitution table with number V and to perform substitution in the subblock with value b. In the considered case, assignment of the dependence of the substitution tables on the value of the binary vector and performance of the substitution operation are accomplished by the microprocessor very quickly during selection of the corresponding values of parameters L and k, for example, when L = 5 and k = 8. With the indicated parameters for positioning of the substitution tables, 8 kbyte of working memory is required, which is acceptable, since modern computers have a volume of working memory many orders of magnitude greater than this value (from 1 to 64 Mbyte and more).

The possibility of technical implementation of the claimed method is explained by the following specific examples of its accomplishment.

Example 1

Let L = 5 and k = 8; these give 32 tables, assigning substitution operations over 8-bit data subblocks. The tables we will assume to be known, i.e., the person attempting to perform cryptanalysis knows these tables. We form a secret key, represented in the form of a group of 8R 16-bit subkeys

$q_{10} \cdot q_{11} \ldots q_{17}$ (first line of subkeys)

$q_{20} \cdot q_{21} \ldots$ 427 (second line of subkeys)

$q_{10} \cdot q_{r1} \ldots q_{r7}$ (r-th line of subkeys)

4RO . q_{R1} ... 4R7 (R-th line of subkeys), where R is the number of encryption rounds

In the r-th round of encryption, the r-th line of subkeys is used.

We denote the employed substitution tables as follows TO, T_1, T_2 ... T31, and the substitution operation assigned by table T_v as S_v, where v = 0, 1, 2. 31 substitution tables T_0, T_1, T_2, T_{15} can be chosen arbitrarily and tables T_{16}, T_{17} ... T_{31} chosen so that the substitution operations S_v and S_{31-v} are mutually inverse. The latter condition is fulfilled, if the pairs of tables T_{16} and T_{15}, T_{17} and T_{14}, T_{18} and T_{13}, T31 and T_0 will assign mutually inverse substitution

operations. For the set of arbitrary substitution tables T_0, T_1, T_2, T_5, it is easy to compile tables corresponding to the inverse substitution operations. For example, for the substitution operation assigned by the following table

0 1 2 255

a_0 a_1 a_2 a_{255},

while the inverse substitution is assigned by the table

0 1 2 255

2_0 [Should be Z_0 - Translator], Z_1 Z_2 2255,

where the line (Z_0, Z_1, Z_2, Z_{255}) is obtained as the upper line after ordering of the columns of the preceding table in the order of increasing numbers in the lower line.

Figure 2 shows a scheme of the arc encryption round, where the solid vertical line corresponds to transmission of 16-bit data subblocks, the dashed line corresponds to transmission of a binary vector V, formed as a function of the value of one of the subblocks being converted, the horizontal solid line corresponds to transmission of a 16-bit subkey. The two-place operation performed over the subblock and subkey, designation of the block, in which the symbol ("•") indicates a two-place operation, formed in the stage of formation of the encryption algorithm and established as one of the following operations "⊕", "+" or "-". The subscript in the symbol "•" denotes the number of the two-place operation.

The one-place operation, performed over the subblock and formed in the stage of formation of the encryption algorithm, is denoted by the block, in which the symbol "<<<C" is indicated. This one-place operation is established as a cyclic shift operation to the left from the number of bits equal to the value of parameter C. In all, 16 different types of cyclic shift operations to the left are possible, which are determined by the value of the parameter C = 0, 1, 2 ... 16. The subscript in parameter C denotes the number of the one-place operation. All the reserved operations "1", "2", "8R-1", "8r" and "<<<C_1" "<<<C_2", "<<<C_{8R-1}", "<<<C_{8R}" are formed as a function of the secret key and the sequential number. For the number of encryption lines equal to R = 4, $3^{8R}16^{8R} = 48^{8R} - 48^{32}$ (about 10^{53}) different modifications of the encryption algorithm are potentially performable. Choice of the specific modification is determined by the choice of the secret key. This number of modifications is fairly high, which determines the uniqueness of the encryption algorithm for each user (or pair of users, using the same secret key for transmission of information along communication lines).

Block S denotes the operation of substitution, performed as a function of the input block according to the table with number V q_{r0}, q_{r1}, q_{r7} – subkeys used in the r-th round. The arrows on the lines denote the direction of transmission of the signals.

Example 1 corresponds to encryption of blocks of digital data with a dimension of 128-bits. Encryption is performed as follows. The input block is broken down into 8 subblocks b_0, b_1 ... b_7 with a size of 16-bit each. After this, in the first round (r = 1), a one-place operation "<<<C_1" is accomplished over subblock b_0, then over subblock bo, and with subkey q_{10} the two-place operation V is performed, the binary vector V is formed, having a value of 5 younger binary digits of subblock b_0 V < - b_0 mod 2^5.

After this, conversion of subblock b_1 is performed. The operation "<<<C_2" b_1 < - b_1 <<<C_2 is performed. Then over b_1 and with subkey q_{11}, the operation "2" is performed, and the output value of this operation is assigned to block V_1, which can be written analytically b_1 < - b_1 *2 q_{11}. Then according to the substitution table with number V, the substitution operation is performed over subblock b_1 b_1 < - S_v (b_1). Then according to the value b_1, the binary vector V is formed (for conversion of the next subblock) V < - b_1 mod 2^5. After this, conversion of subblock b_2 b_2 < - b_2 <<<C_3 . b_2 < - b_2 *3 412, and then b_2 < - S_v(b_2). Similarly, conversions of the subblocks b_3, b_4, b_5, b_6 and b_7 are carried out. In the last step of each round of encryption, rearrangement of the subblocks in inverse order is carried out, i.e., blocks b_7 and b_0, b_6 and b_1, b_5 and b_2, b_4 and b_3 change places in pairs. The second round is performed similarly, except for the fact that, instead of the first line of the subkeys, the second line of the subkeys is used. The third encryption round is then performed, using the third line of the subkeys, etc. In all, R rounds of encryption are carried out, where R = 4. The next algorithm represents a logic form for writing example 1.

Algorithm 1

Input 128-bit input block of digital data, represented as a concatenation of 16-bit subblocks

$b_0|b_1|b_2|b_3|b_4|b_5|b_6|b_7$, where the "|" denotes the concatenation operation

1 Determine the number of encryption rounds R = 4 and counter of the number of rounds R = 1

2 Determine counter i = 1

3 Convert subblock bo bo < - bo <<<C_{Br7}.

bo < - bo*$_{8r-7}$ q_{ro}

4 Form the binary vector V V < - b_{i-1} mod 2^5

5 Convert the subblock b_1 b_1 < - b_1 <<<C_{8R-7+1}

b_1<C_{8r-7+1}

b_1 < - $^1S_v(b_1)$, where the substitution operation ^1S_v is performed with the substitution table with number V

6 Form the binary vector V V < - b_1 mod 2^5

7 If i ≠ 7, then increase i < - i+$_1$ and go to point 5

8 If r ≠ R, then increase r < - r+1, otherwise go to point 10

9 Switch the subblocks in inverse order and go to point 2

10 STOP

Output 128-bit ciphertext block. The next algorithm describes the decoding procedure.

Algorithm 2

Input 128-bit input block ciphertext [illegible].

1 Establish the number of encryption rounds R = 4 and the counter of the number of rounds r = 1

2 Establish the counter i = 1

3 Form the binary vector V V < - b_{i-1} mod 2^5

4 Store the value b_i and the variable g g < - b_1

5 Convert subblock b_1 b_1 < - $^1S_{31-v}(b_1)$

b_1<-b_1(*)$_{8r'-7+1}q_{r'1}$,

b_0<-b_o>$C_{8r'-7+1}$ $q_{r'0}$,

where

r' = 5 - r ">>>C" – cyclic shift operation to the right by C bit and //illegible// operation, inverse operation //illegible// (in operations "<<<C_x" and ">>>C_x", the values of parameter C with the same subscripts are established equal. In this case, the pair of operations "<<<C_x" and ">>>C_x" is a pair of mutually inverse operations)

6 Form the binary vector v v < - g mod 2^5

7 If i ≠ 7, increase i <- i+1 and go to point 4

8 Convert the subblock bo bo < - bo (*)$_{8r-7}$ q_{r0}

bo < - bo >>>C_{8r-7}

9 If r ≠ R, then increase r < - r+1, otherwise go to point 11

10 Switch the subblocks in reverse order and go to point 2

11 STOP

Output 64-bit block of initial text

During program implementation, algorithm 1 and algorithm 2 that implement the claimed method ensure an encryption rate of about 30 Mbit/s for Pentium 200 microprocessors. If necessary, a different number of rounds can be assigned, for example, R = 2, 3, 5, 6.

Example 2

This example is similar to example 1, the only difference being that the employed 32 substitution tables are secret, for example, they are formed as a function of a secret key. This variant is easy to implement during use of a computer for encryption of data by formation of substitution tables with a special program during input of a secret key to the encryption module. Formation of the secret tables can be accomplished, for example, by modifying the known (previously assigned) substitution tables by block encryption according to a secret key of elements of the lower line of the known tables (since block encrypting conversion is a substitution, the modified tables will also be substitution tables).

Example 3

This example is also similar to example 1 and is explained in Figure 3. The only difference is that, instead of the formed substitution operation $^{1}S_{v}$, one-place conversion operations are used that depend on the binary vector V (V, in turn, depends on the input block of digital data), which are denoted as "(<S<)" and are formed in the stage of formation of the encryption algorithm. Subscript j denotes the number of the position of the operation "(<S<)". The operations "(<S<)" are established as a function of the values of j (j = 1, 2, 7R, where R is the number of encryption rounds) and under secret key as one of the following five operations "$^{1}S_{v}$", "$^{2}S_{v}$", "$<<<_{2}V$", "$<<<_{3}V$", "$<<<_{4}V$". All the listed operations are dependent on the input block. Each of the given operations is performed as a function of the converted data block, since it depends on the binary vector V. If, in a certain position originally reserved under the operation "(<S<)", a substitution operation is established, then it is performed according to a table with number V, if a cyclic shift operation is established, it is performed with a cyclic shift by V-bit. The number of possible modifications of the encryption algorithm in the given example is 5^{7R} times greater than in example 1, which amounts to about 10^{75}, where R = 4.

Example 4

This example is similar to example 3, the only difference being that the employed 32 substitution tables are secret, for example, they are formed as a function of the secret key. This variant requires compilation of a more complex program for formation of the encryption algorithm, but it permits an increase in cryptographic integrity of encryption with retention of high encryption rate.

The cited examples demonstrate that the proposed method for cryptographic conversions of blocks of digital data can be technically implemented and permits solution to the posed problem.

The claimed method can be implemented, for example, on personal computers, and ensures the possibility of creating on its basis high-speed program modules for encryption and replacement of costly specialized encryption equipment with a personal computer equipped with a program system for high-speed encryption.

Claims

1. Method for encryption of blocks of digital data, consisting of formation of a secret key, breakdown of the data block into N>2 subblocks and sequential conversion of the subblocks by accomplishing on the i-th subblock at least one conversion operation, which depends on the value of the j-th subblock, where $j \neq i$, characterized by the fact that, after formation of the secret key, the encryption algorithm is additionally formed as a function of a secret key by formation of at least one conversion operation that is accomplished on the i-th subblock as a function of the j-th subblock.

2. Method according to Claim 1, characterized by the fact that the conversion operation is formed in the form of a substitution operation.

(19) RU (11) 2 124 814 (13) C1

(51) МПК[6] H 04 L 9/00

РОССИЙСКОЕ АГЕНТСТВО
ПО ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ РОССИЙСКОЙ ФЕДЕРАЦИИ

(21), (22) Заявка 97121649/09, 24.12.1997

(46) Дата публикации 10.01.1999

(56) Ссылки RU 94032780 A1, 20 07 96. RU 2032990 C1, 10.04.95. EP 0406187 A1, 02.01.92. WO 91/00661 A1, 10.01.91.

(98) Адрес для переписки
197022 Санкт-Петербург, ул.Кантемировская 10, СЦПС "СПЕКТР"

(71) Заявитель
Молдовян Николай Андреевич,
Молдовян Александр Андреевич,
Государственное унитарное предприятие Специализированный центр программных систем "СПЕКТР"

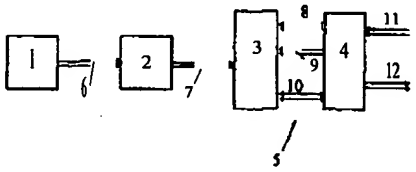
(72) Изобретатель Молдовян А.А., Молдовян Н.А., Молдовяну П.А.

(73) Патентообладатель
Молдовян Николай Андреевич,
Молдовян Александр Андреевич,
Государственное унитарное предприятие Специализированный центр программных систем "СПЕКТР"

(54) СПОСОБ ШИФРОВАНИЯ БЛОКОВ ЦИФРОВЫХ ДАННЫХ

(57) Реферат

Изобретение относится к области электросвязи и вычислительной техники, а конкретнее к области криптографических способов и устройств для шифрования цифровых данных Способ заключается в формировании секретного ключа, разбиении блока данных на N > 2 подблоков и поочередном преобразовании подблоков путем осуществления над i-тым подблоком по крайней мере одной операции преобразования, которая зависит от значения j-го подблока, где $j \neq i$, причем после формирования секретного ключа дополнительно формируют алгоритм шифрования в зависимости от секретного ключа путем формирования по крайней мере одной операции преобразования, которую осуществляют над i-тым подблоком в зависимости от j-го подблока, а операцию преобразования формируют в виде операции подстановки, при этом достигается технический результат, состоящий в повышении стойкости к известным методам криптоанализа, включая дифференциальный и линейный криптоанализ 1 з п ф-лы, 3 ил



Фиг, 1.

RU 2124814 C1

RU 2124814 C1

(19) **RU** (11) **2 124 814** (13) **C1**

(51) Int. Cl.[6] **H 04 L 9/00**

RUSSIAN AGENCY FOR PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: **97121649/09, 24.12.1997**

(46) Date of publication: 10.01.1999

(98) Mail address:
197022 Sankt-Peterburg, ul.Kantemirovskaja 10, STsPS "SPEKTR"

(71) Applicant:
Moldovjan Nikolaj Andreevich, Moldovjan Aleksandr Andreevich, Gosudarstvennoe unitarnoe predprijatie Spetsializirovannyj tsentr programmnykh sistem "SPEKTR"

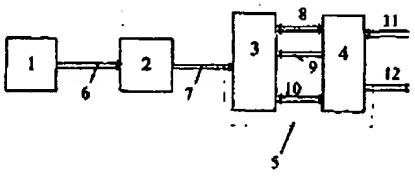
(72) Inventor. **Moldovjan A.A., Moldovjan N.A., Moldovjanu P.A.**

(73) Proprietor.
Moldovjan Nikolaj Andreevich, Moldovjan Aleksandr Andreevich, Gosudarstvennoe unitarnoe predprijatie Spetsializirovannyj tsentr programmnykh sistem "SPEKTR"

(54) METHOD FOR ENCODING OF DIGITAL DATA

(57) Abstract:

FIELD: communication, computer engineering, in particular, cryptography. SUBSTANCE: method involves generation of secret key, splitting data records into N blocks, and sequential conversion of blocks by running at least one conversion for i-th block, depending on value of j-th block, where j is not equal to i. In addition after generation of secret key method involves generation of encryption algorithm depending on value of secret key by running at least one conversion operation over i-th block Said conversion operation is designed as substitution EFFECT: increased resistance to known methods of cryptanalysis, including differential and linear cryptanalysis. 2 cl, 3 dwg



Фиг. 1.

RU 2124814 C1

RU 2124814 C1

Изобретение относится к области электросвязи и вычислительной техники, а конкретнее к области криптографических способов и устройств для шифрования сообщений (информации) В совокупности признаков заявляемого способа используются следующие термины

- секретный ключ представляет собой двоичную информацию, известную только законному пользователю,

- подключ - элемент секретного ключа, представленного как совокупность подключей,

- шифрование есть процесс преобразования информации, который зависит от секретного ключа и преобразует исходный текст в шифртекст, представляющий собой псевдослучайную последовательность знаков, из которой получение информации без знания секретного ключа практически неосуществимо

- дешифрование есть процесс, обратный процедуре шифрования, дешифрование обеспечивает восстановление информации по криптограмме при знании секретного ключа,

- шифр представляет собой совокупность элементарных шагов преобразования входных данных с использованием секретного ключа, шифр может быть реализован в виде программы для ЭВМ или в виде отдельного устройства,

- криптоанализ - метод вычисления секретного ключа для получения несанкционированного доступа к зашифрованной информации или разработка метода, обеспечивающего доступ к зашифрованной информации без вычисления секретного ключа,

- криптоаналитик - лицо, выполняющее криптоанализ, т е атакующее шифр,

- криптостойкость является мерой надежности защиты зашифрованной информации и представляет собой трудоемкость, измеренную в количестве элементарных операций, которые необходимо выполнить для восстановления информации по криптограмме при знании алгоритма преобразования, но без знания секретного ключа, в случае односторонних преобразований под криптостойкостью понимается сложность вычисления входного значения блока по его выходному значению,

- операции циклического сдвига, зависящие от преобразуемых подблоков или зависящие от двоичного вектора - это операции циклического сдвига на число бит, задаваемое значением подблока или значением двоичного вектора, операции циклического сдвига влево (вправо) обозначаются знаком " <<<" (">>>"), например, запись $B_1<B_2$ обозначает операцию циклического сдвига влево подблока B_1 на число бит, равное значению двоичного вектора B_2.

- одноместная операция - это операция, выполняемая над одним операндом (блоком данных или двоичным вектором), значение подблока после выполнения некоторой данной одноместной операции зависит только от его начального значения, примером одноместных операций являются операции циклического сдвига,

- двухместная операция - это операция, выполняемая над двумя операндами, результат выполнения некоторой данной двухместной операции зависит от значения каждого операнда, примером двухместных операций являются операции сложения, вычитания, умножения и др ,

- наложение подключа на подблок - это процедура выполнения двухместной операции (*) над подблоком (B) и подключом (Q) и присваивания результата выполнения этой операции подблоку, что аналитически записывается в виде формулы B <- B*Q, где " <- " - знак операции присваивания

Известны способы блочного шифрования данных, см , например, стандарт США DES [National Bureau of Standards Data Encryption Standard Federal Information Processing Standards Publication 46, January 1977, см также С Мафтик Механизмы защиты в сетях ЭВМ - М , Мир, 1993 С 42-47] В данном способе шифрование блоков данных выполняют путем формирования секретного ключа, разбиения преобразуемого блока данных на два подблока L и R и поочередного изменения последних путем выполнения операции поразрядного суммирования по модулю два над подблоком L и двоичным вектором, который формируется как выходное значение некоторой функции F от значения подблока R После этого блоки переставляются местами Функция F в указанном способе реализуется путем выполнения операций перестановки и подстановки, выполняемых над подблоком R Данный способ обладает высокой скоростью преобразований при реализации в виде специализированных электронных схем

Однако известный способ-аналог использует секретный ключ малого размера (56 бит), что делает его уязвимым к криптоанализу на основе подбора ключа Последнее связано с высокой вычислительной мощностью современных ЭВМ массового применения

Наиболее близким по своей технической сущности к заявляемому способу криптографического преобразования L-битовых входных блоков цифровых данных в L-битовые выходные блоки является способ, реализованный в шифре RC5, описанный в работе R Rivest, The RC5 Encryption Algonthm/ Fast Software Encryption, Second International Workshop Proceedings (Leuven, Belgium, December 14-16, 1994), Lecture Notes in Computer Science, v 1008, Springer-Verlag, 1995, pp 86-96 Способ-прототип включает в себя формирование секретного ключа в виде совокупности подключей, разбиение входного блока данных на подблоки A и B и поочередное преобразование подблоков Подблоки преобразуются путем выполнения над ними одноместных и двухместных операций В качестве двухместных операций используются операции сложения по модулю 2^n, где n = 8, 16, 32, 64, и операция поразрядного суммирования по модулю 2 В качестве одноместной операции используется операция циклического сдвига влево, причем число бит, на которое сдвигается преобразуемый подблок, зависит от значения другого подблока, это определяет зависимость операции циклического сдвига на текущем шаге преобразования подблока от исходного значения входного блока данных Двухместная операция выполняется над подблоком и подключом, а также над двумя

RU 2124814 01

RU 2124814 01

подблоками Характерным для способа-прототипа является использование операции циклического сдвига, зависящей от значения входного блока

Подблок, например подблок B, преобразуют следующим путем Выполняется операция поразрядного суммирования по модулю 2 над подблоками A и B и значение, получаемое после выполнения этой операции, присваивается подблоку B Это записывается в виде соотношения B ←_ B⊕V, где знак " <- " - обозначает операцию присваивания и знак " ⊕ " обозначает операцию поразрядного суммирования по модулю 2 После этого над подблоком B выполняют операцию циклического сдвига на число бит, равное значению подблока A B <- B<<<A Затем над подблоком и одним из подключеи S выполняют операцию суммирования по модулю 2^n, где n - длина подблока в битах B <- B+S mod 2^n После этого аналогичным образом преобразуется блок A Выполняется несколько таких шагов преобразования обоих подблоков

Данный способ обеспечивает высокую скорость шифрования при реализации в виде программы для ЭВМ Однако способ-прототип имеет недостатки, а именно, при программной реализации для ЭВМ с 32-разрядным микропроцессором он не обеспечивает высокой стойкости криптографического преобразования данных к дифференциальному и линейному криптоанализу [Kaliski B S , Yin Y L On Differential and Linear Cryptanalysis of the RC5 Encryption Algorithm Advances in Cryptology - CRYPTO '95 Proceedings, Springer-Verlag, 1995, pp 171-184] Этот недостаток связан с тем, что эффективность использования операций зависящих от преобразуемых данных с целью усложнения известных методов криптоанализа снижается тем, что алгоритм шифрования известен криптоаналитику, что позволяет последнему выявить статистические особенности процедур шифрования и использовать их при проведении криптоанализа

В основу изобретения положена задача разработать способ шифрования блоков цифровых данных, в котором шифрование входных данных осуществлялось бы таким образом, чтобы выявления статистических особенностей алгоритма шифрования криптоаналитиком было бы существенно затруднено, благодаря чему повышается стойкость к известным методам криптоанализа, включая дифференциальный и линейный криптоанализ

Поставленная задача достигается тем, что в способе криптографического преобразования блоков цифровых данных, заключающемся в формировании секретного ключа, разбиении блока данных на N>2 подблоков и поочередном преобразовании подблоков путем осуществления над подблоком по крайней мере одной операции преобразования, которая зависит от значения входного блока, новым согласно изобретению является то, что после формирования секретного ключа дополнительно формируют алгоритм шифрования в зависимости от секретного ключа

Благодаря такому решению обеспечивается существенное усложнение выявления статистических особенностей алгоритма шифрования криптоаналитиком, благодаря чему обеспечивается повышение стойкости криптографического преобразования к известным методам криптоанализа

Новым является также то, что один из подблоков дополнительно преобразуют путем осуществления над ним операции подстановки, которая зависит от входного блока и выполняется по секретным таблицам подстановок Благодаря такому решению обеспечивается дополнительное повышение криптостойкости к известным методам криптоанализа

Новым является также то, что алгоритм шифрования формируют путем формирования операций, которые зависят от входного блока

Благодаря такому решению, обеспечивается дополнительное повышение криптостойкости к известным методам криптоанализа Новым является также то, что алгоритм шифрования формируют путем формирования операций подстановок, которые зависят от входного блока и осуществляются по секретным таблицам подстановок

Благодаря такому решению, обеспечивается дополнительное повышение криптостойкости к известным методам криптоанализа

Ниже сущность заявляемого изобретения более подробно разъясняется примерами его осуществления со ссылками на прилагаемые чертежи

На фиг 1 представлена обобщенная схема криптографического устройства для шифрования блоков цифровых данных в соответствии с заявляемым способом

На фиг 2 представлена схема шифрования, соответствующая примеру 1

На фиг 3 представлена схема шифрования, соответствующая примеру 3

Заявляемый способ может быть реализован с помощью ЭВМ или вычислительного устройства, представленного блок-схемой на фиг 1, где

блок 1 - устройство ввода секретного ключа,

блок 2 - блок формирования машинного кода программы шифрования (блок настройки шифра),

блок 3 - блок памяти устройства шифрования,

блок 4 - операционный блок устройства шифрования, содержащий три, четыре или более регистра,

блок 5 - устройство шифрования,

6 - шина передачи информационных сигналов секретного ключа пользователя,

7 - шина передачи информационных сигналов сформированного машинного кода программы шифрования и секретного ключа,

8 - шина передачи информационных сигналов подключей и передачи информационных сигналов входных данных и информационных сигналов преобразуемых подблоков,

9 - шина адресации,

10 - шина передачи информационных сигналов машинного кода программы шифрования,

11 - шина ввода входных данных,

12 - шина вывода шифртекста

RU 2124814 C1

RU 2124814 C1

Формирование секретного ключа можно осуществить непосредственно вводя его в шифрующую систему или оперативную память ЭВМ, например, со съемного носителя информации Входной блок данных разбивают на подблоки, например, путем представления подблока в виде совокупности подблоков, записанных по фиксированным адресам в блок памяти 3.

Используя блок 1 вводят секретный ключ, информационный сигнал которого по шине 6 подают на вход блока 2. В блоке 2 формируют в зависимости от секретного ключа алгоритм шифрования, т. е генерируют машинный код программы шифрования под управлением секретного ключа. При этом формирование алгоритма шифрования осуществляют таким образом, чтобы любая модификация алгоритма шифрования включала разбиение блока цифровых данных на подблоки и поочередное преобразование подблоков путем осуществления двухместной операции над подблоком и подключом и выполнения над подблоком операции преобразования, зависящей от входного блока.

Информационный сигнал секретного ключа и информационный сигнал машинного кода программы шифрования по шине 7 передают в блок памяти 3. После этого устройство шифрования 5 содержит в памяти секретный ключ и машинный код, реализующий сформированный алгоритм шифрования, и готово к выполнению операций шифрования Данное инициализированное состояние устройства сохраняется в течение всего времени работы законного пользователя. Входной блок цифровых данных вводят по шине 11 в операционный блок 4 и затем по шине 8 в блок памяти 3 Блок шифртекста считывается с шины 12 По шине 10 в операционный блок 4 передают коды машинных команд для выполнения процедур преобразования. При завершении работ по шифрованию данных пользователь выключает устройство шифрования, что приводит к автоматическому стиранию секретного ключа и сформированного машинного кода алгоритма шифрования из области памяти блока 2 и блока 3, поскольку отключается электропитание всех блоков устройства шифрования. Таким образом, конкретная модификация алгоритма шифрования также как и секретный ключ являются недоступными для потенциального криптоаналитика, которому известен только алгоритм формирования алгоритма шифрования Это существенно затрудняет выявление статистических особенностей конкретной модификации алгоритма шифрования При числе потенциально реализуемых модификаций, равном или более 10^{20}, заявляемый способ шифрования обеспечивает высокую стойкость ко всем известным методам криптоанализа.

Формирование алгоритма шифрования может быть осуществлено следующим образом. Предварительно на основе одного из известных алгоритмических языков составляется программа-шаблон В программе-шаблоне зарезервированы места, в которых предусмотрена возможность записи любой из некоторого набора операций (например, двухместных операций или операций циклического сдвига, зависящих от входного блока). Все зарезервированные места (под операции преобразования) нумеруют. Поочередно, начиная с первого, для всех зарезервированных мест формируют операции преобразования в зависимости от значения элемента дополнительной псевдослучайной последовательности, имеющего номер, совпадающий с номером настраиваемой операции Генерацию псевдослучайной последовательности необходимой длины осуществляют в зависимости от секретного ключа, например, используя генераторы псевдослучайных чисел, описанные в работе Брикелл Э Ф., Одлижко Э.М. Криптоанализ: Обзор новейших результатов// ТИИЭР. 1988 Т 76. N. 5. С. 87-89

Формирование операций преобразования осуществляют, например, следующим образом Двухместная операция, используемая для наложения подключа на подблок, устанавливается как операция поразрядного суммирования по модулю два ($\oplus$), если $d_j \bmod 3 = 0$, где dj - значение соответствующего элемента дополнительной псевдослучайной последовательности, либо как операция суммирования по модулю 2^{32} (+), если $d^j \bmod 3 = 1$, либо как операция вычитания по модулю 2^{32} (-), если $d_j \bmod 3 = 2$. В процедурах настройки алгоритма дешифрования настраиваются операции, являющиеся обратными по отношению к соответствующим операциям, настраиваемым в алгоритме шифрования. Для этого бинарная операция в алгоритме дешифрования устанавливается как операция поразрядного суммирования по модулю два (Ф), если $d\,j \bmod 3 = 0$, либо как операция вычитания по модулю 2^{32} (-), если $d_j \bmod 3 = 1$, либо как операция суммирования по модулю 2^{32} (+), если $dj \bmod 3 = 2$

После того, как в программе шифрования, записанной на алгоритмическом языке (например, на языке СИ или Паскаль), установлены операции преобразования во всех зарезервированных местах, генерируется машинный код, соответствующий программе шифрования, используя, например, транслятор, преобразующий программу, составленную на алгоритмическом языке, в последовательность машинных команд. Секретный ключ и машинный код программы шифрования записываются в оперативную память ЭВМ (или специализированного шифрующего устройства) и находятся там постоянно в течение всего времени работы данного пользователя, выполняя преобразование поступающих для шифрования блоков данных. Сложность процедур формирования ключа шифрования и генерирования машинного кода программы шифрования не влияет на скорость шифрования, поскольку эту процедуру выполняют однократно при идентификации пользователя по паролю в момент включения шифрующего устройства или вызова шифрующей программы

Дополнительное повышение криптостойкости шифрования достигается при задании формирования операций преобразования, зависящих от преобразуемых данных Например, для позиции, зарезервированной под

RU 2124814 C1

RC 2124814 C1

одноместную операцию над одним из преобразуемых 32-битовых подблоков - подблоком B_i, можно задать формирование одной из следующих операций: (1) операции (^1S_v) подстановки над 8 младшими двоичными разрядами (с номерами от 1-го по 8-й) подблока, выполняемая по V-той таблице подстановки, номер которой выбирается в зависимости от подблока Bj, где $i \neq j$, (2) аналогичной операции (^2S_v) подстановки над двоичными разрядами подблока с номерами от 9-го до 16-го включительно, (3) операции ($<<<_1V$) циклического сдвига влево содержимого подблока на число бит, равное $V = B_j \bmod 32$, где $i \neq j$, (4) операции ($<<<_2V$) циклического сдвига влево содержимого младших 16 двоичных разрядов подблока на число бит, равное $V = Bj \bmod 16$, где $i \neq j$, (5) операции ($<<<_3V$) циклического сдвига влево содержимого младших 8 двоичных разрядов подблока на число бит, равное значению $V = B_j \bmod 8$, где $i \neq j$, (6) операции ($<<<_4V$) циклического сдвига влево содержимого двоичных разрядов с 9-го по 16-й включительно подблока на число бит, равное значению V = Bj mod 8, где fetj

После того, как в программе шифрования, записанной на алгоритмическом языке (например, на языке СИ или Паскаль), установлены операции преобразования во всех зарезервированных местах, генерируется машинный код, соответствующий программе шифрования, используя, например, транслятор, преобразующий программу, составленную на алгоритмическом языке, в последовательность машинных команд. Секретный ключ и машинный код программы шифрования записываются в оперативную память ЭВМ (или специализированного шифрующего устройства) и находятся там постоянно в течение всего времени работы данного пользователя, выполняя преобразование поступающих для шифрования блоков цифровых данных

Сложность процедур формирования ключа шифрования и генерирования машинного кода программы шифрования не влияет на скорость шифрования, поскольку эту процедуру выполняют однократно при идентификации пользователя по его секретному ключу в момент включения шифрующего устройства или вызова шифрующей программы. На современных ЭВМ процедура формирования алгоритма шифрования в виде машинного кода программы шифрования легко может быть автоматизирована и реализована в виде программы инициализации модуля шифрования. Время, необходимое для выполнения программы инициализации, составляет от 0,03 до 0,5 секунд в зависимости от конкретного варианта реализации заявляемого способа, что приемлемо для большинства применений систем защиты информации

Аналогичным способом формируется программа дешифрования блоков криптограммы Шифрующая и соответствующая ей дешифрующая программы составляют единую криптографическую программу. Машинный код криптографической программы записывается в оперативную память ЭВМ, которая под его управлением выполняет процедуры шифрования и дешифрования блоков. Процедуры шифрования и ключ шифрования сформированы в зависимости от секретного ключа (пароля) пользователя, т е. являются уникальными, что обеспечивает высокую сложность криптоанализа

Важным типом операций, зависящих от преобразуемых данных, являются операции подстановок, осуществляемые по таблицам, выбираемым в зависимости от входного блока. Пусть операции подстановки выполняются над подблоками цифровых данных длиной k бит, где k - целое число. Тогда для задания операции подстановки, преобразующей k-битовый входной подблок в k-битовый выходной подблок, требуется использование таблицы, содержащей две строки чисел.

0 1 2 ... N-1

$a_0\ a_1\ a_2 \ldots a_{N-1}$,

где

$N = 2^k$

В данной таблице в нижней строке присутствуют все возможные значения k-битового блока ровно по одному разу, но в произвольном порядке Очередность расположения чисел в нижней строке определяет конкретный вариант таблицы подстановки, а следовательно, и конкретный вариант операции подстановки, выполняемой с использованием этой таблицы. Выполнение операции подстановки осуществляется следующим образом. Выбирается в верхней строке число, которое равно значению входного блока. Находящееся под этим числом значение в нижней строке берется в качестве выходного блока Таким образом, таблицу подстановки можно разместить в оперативной памяти ЭВМ как последовательную запись k-битовых компьютерных слов, размещенных в ячейках с адресами $W_0, W_1, W2, \ldots, W_{N-1}$. В этом случае значение входного блока b служит для вычисления адреса W o + b слова, которое берется в качестве выходного блока. Этот способ представления таблицы подстановки требует использования объема памяти, равного kN бит.

Выберем количество таблиц подстановки, равное 2^L (объем требуемой памяти составит при этом $2^L kN$ бит), и разместим таблицы подстановок непрерывно друг за другом В качестве адреса таблицы с номером V возьмем значение адреса W_0 ее первого k-битового слова. Пусть адрес таблицы с номером 0 есть s. В этом случае адрес таблицы подстановки с произвольным номером V равен s + VN. Если заданы номер текущей таблицы подстановки V и текущий входной подблок для выполнения операции подстановки, то она выполняется заменой текущего входного блока на k-битовое слово, расположенное по адресу s + VN + b, где b - значение подблока, над которым выполняется текущая операция подстановки. Используя это соотношение легко задать выбор таблицы подстановки с номером V и выполнить подстановку над подблоком со значением b В рассмотренном случае задание зависимости таблиц подстановок от значения двоичного вектора и выполнение операции подстановки осуществляются микропроцессором очень

RU 2124014 C1

RU 2124014 C1

быстро при выборе соответствующих значений параметров L и k, например при L - 5 и k = 8 При указанных параметрах для размещения таблиц подстановки требуется 8 Кбайт оперативной памяти, что является приемлемым, поскольку современные ЭВМ обладают объемом оперативной памяти на многие порядки больше этой величины (от 1 до 64 Мбайт и более)

Возможность технической реализации заявляемого способа поясняется следующими конкретными примерами его осуществления

Пример 1

Пусть L=5 и k=8, те даны 32 таблицы, задающие операции подстановки над 8-битовыми подблоками данных Таблицы будем предполагать известными, т е лицо, пытающееся провести криптоанализ, знает эти таблицы Сформируем секретный ключ, представленный в виде совокупности из 8R 16-битовых подключей

q_{10}, q_{11} . . q_{17} (первая строка подключей)

q_{20}, q_{21}, . . 427 (вторая строка подключей)

q_{r0}, q_{r1}, , q_{r7} ((r-тая строчка подключей)

4RO. q_{R1}, , 4R7 (R-тая строка подключей),

где R - число раундов шифрования

На г-том раунде шифрования используется г-тая строка подключей

Обозначим используемые таблицы подстановки следующим образом TO, T_1, T_2, ,Тз1, а операцию подстановки, задаваемую таблицей T_v, как S_v, где v = 0, 1, 2, , 31 Таблицы подстановок T_0, T_1, T_2 ,T_{15} могут быть выбраны произвольными, а таблицы T_{16}, T_{17}, , T_{31} берутся такими, чтобы операции подстановок S_v и S_{31-v} были взаимно обратными Последнее условие выполняется, если пары таблиц T_{16} и T_{15}, T_{17} и T_{14} T_{18} и T_{13}, , Тз1 и T_0 будут задавать взаимно обратные операции подстановки Для набора произвольных таблиц подстановки T_0, T_1, T_2, .T_5 легко составить таблицы, соответствующие обратным операциям подстановки Например, для операции подстановки, задаваемой следующей таблицей

0 1 2 255

$a_0\ a_1\ a_2$ a_{255},

а обратная подстановка задается тэблицей

0 1 2 255

$2_0\ Z_1\ Z_2$ 2255.

где строка (Z_0, Z_1, Z_2, , Z_{255}) получается как верхняя строка после упорядочения столбцов предыдущей таблицы в порядке возрастания чисел в нижней строке

На фиг 2 показана схема г-го раунда шифрования, где сплошная вертикальная линия соответствует передаче 16-битовых подблоков данных, пунктирная линия соответствует передаче двоичного вектора V, формируемого в зависимости от значения одного из преобразуемых подблоков, горизонтальнэя сплошная линия соответствует передаче 16-битового подключа Двухместная операция, выполняемая над подблоком и подключом, обозначена блоком, в котором указан знак ("*") двухместной операции, формируемой на этапе формирования алгоритма шифрования и устанавливаемой как одна из следующих операций "⊕", "+" или "-" Нижний индекс у знака "*" обозначает номер двухместной операции

Одноместная операция, выполняемая над подблоком и формируемая на этапе формирования алгоритма шифрования, обозначена блоком в котором указан знак " <<<C" Данная одноместная операция устанавливается как операция циклического сдвига влево на число бит равное значению параметра C Всего возможны 16 разных типов операций циклического сдвига влево, которые определяются значением параметра C = 0 1, 2, , 16 Нижний индекс у параметра C обозначает номер одноместной операции Все зарезервированные операции "*1", "*2", ."*8R-1", "*8R" и "<<<C_1", " <<<C_2", ."<<<C_{8R-1}", "<<<C_{8R}" формируются в зависимости от секретного ключа и от порядкового номера Для числа раундов шифрования, равного R = 4, потенциально реализуемы $3^{8R}16^{8R} = 48^{8R} - 48^{32}$ (около 10^{53}) различных модификаций алгоритма шифрования Выбор конкретной модификации определяется выбором секретного ключа Данное число модификаций достаточно велико, что определяет уникальность алгоритма шифрования для каждого пользователя (или пары пользователей, использующих одинаковый секретный ключ для передачи сообщений по линиям связи)

Блок S обозначает операцию подстановки, выполняемую в зависимости от входного блока по таблице с номером V q_{r0}, q_{r1}, , q_{r7} - подключи, используемые на г-ом рэунде Стрелки нз линиях обозначэют направление передачи сигналов

Пример 1 соответствует шифрованию блоков цифровых данных размером 128 бит Шифрование выполняют следующим путем Входной блок разбивают на 8 подблоков b_0, b_1, , b7 размером 16 бит каждый После этого на первом раунде (r=1) над подблоком b_0 осуществляют одноместную операцию "<<<C_1", затем над подблоком bo и подключом q_{10} выполняют двухместную операцию "V, формируют двоичный вектор V, имеющий значение 5 младших двоичных разрядов подблока b_0 V <- b_0 mod 2^5

После этого выполняют преобразование подблока b_1 Над подблоком b_1 выполняют операцию "<<<C_2" b_1 <- b_1 <<<C_2 Затем над b_1 и подключом q_{11} выполняют операцию "*2" и выходное значение этой операции присваивают блоку b_1, что можно записать аналитически следующим образом b_1 <- b 1 *2 q_{11} Затем по таблице подстановки с номером v выполняют операцию подстановки над подблоком b_1 b_1 <- S_v (b_1) Затем по значению b_1 формируют двоичный вектор V (для преобразования следующего подблока) V <- b_1 mod 2^5 После этого выполняют преобразование подблока Ь2 b_2 <- b_2<<<C_3, b_2 <- b_2 *з 412 и затем b_2<- $S_v(b_2)$ Аналогично выполняют преобразования подблоков b_3, b_4, b_5, b_6 и b_7 На последнем шаге каждого раунда шифрования выполняют перестановку подблоков в обратном порядке, т е попарно меняются местами блоки b 7 и b_0, b_8 и b_1, b_5 и b_2, b_4 и b_3 Второй раунд

RU 2150014 01

RU 2124814 01

выполняется аналогично, за исключением того, что вместо первой строки подключей используется вторая строка подключей Затем выполняется третий раунд шифрования с использованием третьей строки подключей и т д Всего выполняется R раундов шифрования, где R = 4 Следующий алгоритм представляет собой логическую форму записи примера 1

Алгоритм 1

Вход 128-битовый входной блок цифровых данных, представленный как конкатенация 16-битовых подблоков $b_0|b_1|b_2|b_3|b_4|b_5|b_6|b_7$, где знак " | " обозначает операцию конкатенации

1 Установить число раундов шифрования R = 4 и счетчик числа раундов r = 1

2 Установить счетчик i = 1

3 Преобразовать подблок bo bo <- $b_o <<< C_{8r-7}$,

$b_0 <- b_0 *_{8r-7} q_{r0}$

4 Сформировать двоичный вектор V V <- $b_{i-1} \bmod 2^5$

5 Преобразовать подблок b_i b_i <- $b_i <<< C_{8r-7+i}$,

$b_i <- b_i *_{8r-7+i} q_{ri}$,

b_i <- $^1S_v(b_i)$, где операция подстановки ^1S_v выполняется с помощью таблицы подстановки с номером V

6 Сформировать двоичный вектор V V <- $b_i \bmod 2^5$

7 Если i≠7, то прирастить i <- i+1 и перейти к п 5

8 Если r≠R, то прирастить r <- r+1 В противном случае перейти к п 10

9 Переставить подблоки в обратном порядке и перейти к п 2

10 СТОП

Выход 128-битовый блок шифртекста

Следующий алгоритм описывает процедуры дешифрования

Алгоритм 2

Вход 128-битовый входной блок шифртекста $b_0 | b_1 | b_2 | b_3 | b_4 | b_5 | b_6 | b_7$.

.

1 Установить число раундов шифрования R = 4 и счетчик числа раундов r = 1

2 Установить счетчик i = 1

3 Сформировать двоичный вектор V V <- $b_{i-1} \bmod 2^5$

4 Сохранить значение b_i в переменной g g <- b_i

5 Преобразовать подблок b_i b_i <- $^1S_{31-V}(b_i)$

$b_i <- b_i (*)_{8r'-7+i} q_{r'i}$,

$b_0 <- b_0 >>> C_{8r'-7+i}$ $q_{r'0}$,

где

r' = 5 - r, ">>>C" - операция циклического сдвига вправо на C бит и "$(*)_{8r'-7+i}$" - операция, обратная операции "$*_{8r'-7+i}$" (В операциях " $<<<C_x$" и ">>>C_x" значения параметра C с одинаковыми индексами устанавливаются равными В этом случае пара операций "$<<<C_x$" и ">>>C_x" является парой взаимно обратных операций)

6 Сформировать двоичный вектор v v <- g $\bmod 2^5$

7 Если i≠7, то прирастить i <- i+1 и перейти к п 4

8 Преобразовать подблок bo bo <- b o $(*)_{8r'-7}$ $q_{r'0}$

bo <- bo >>>$C_{8r'-7}$

9 Если r≠R, то прирастить r <- r+1 В противном случае перейти к п 11

10 Переставить подблоки в обратном порядке и перейти к п 2

11 СТОП

Выход 64-битовый блок исходного текста

При программной реализации алгоритм 1 и алгоритм 2, реализующие заявляемый способ, обеспечивают скорость шифрования около 30 Мбит/с для микропроцессора Pentium/200 При необходимости может быть задано и другое число раундов, например R = 2, 3, 5, 6

Пример 2

Этот пример является аналогичным примеру 1, а отличие состоит только в том, что используемые 32 таблицы подстановок являются секретными, например они формируются в зависимости от секретного ключа Этот вариант является легко реализуемым при использовании ЭВМ для шифрования данных путем формирования таблиц подстановок с помощью специальной программы при вводе секретного ключа в модуль шифрования Формирование секретных таблиц может быть реализовано, например, путем модифицирования известных (заранее заданных) таблиц подстановки путем блочного шифрования по секретному ключу элементов нижней строки известных таблиц (поскольку блочное шифрующее преобразование является подстановкой, то модифицированные таблицы также будут являться таблицами подстановок)

Пример 3

Данный пример также является аналогичным примеру 1 и поясняется на фиг 3 Отличие состоит в том, что вместо фиксированных операций подстановок ^1S_v используются одноместные операции преобразования, зависящие от двоичного вектора V (V в свою очередь зависит от входного блока цифровых данных), которые обозначены как "(<S<)$_j$" и формируются на этапе формирования алгоритма шифрования Индекс j обозначает номер позиции операции "(<S<)" Операции "(<S<)" устанавливаются в зависимости от значения j (j=1, 2, 7R, где R - число раундов шифрования) и от секретного ключа как одна из следующих пяти операций " ^1S_v", "^2S_v", "$<<<_2V$", "$<<<_3V$", "$<<<_4V$" Все перечисленные операции являются, зависящими от входного блока Каждая из данных операций выполняется в зависимости от преобразуемого блока данных, поскольку она зависит от двоичного вектора V Если в некоторой позиции, первоначально зарезервированной под операцию "(<S<)", установлена операция подстановки, то она выполняется по таблице с номером V, если установлена операция циклического сдвига, то выполняется циклический сдвиг на V бит Число возможных модификаций алгоритма шифрования в данном примере составляет в 5^{7R} раз больше, чем в примере 1, что составляет около 10^{75} при R=4

Пример 4

Этот пример является аналогичным

RU 2124814 01

RU 2124814 01

примеру 3, а отличие состоит только в том, что используемые 32 таблицы подстановок являются секретными, например они формируются в зависимости от секретного ключа Этот вариант требует составления более сложной программы формирования алгоритма шифрования, однако он позволяет повысить криптостойкость шифрования при сохранении высокой скорости шифрования.

Приведенные примеры показывают, что предлагаемый способ криптографических преобразований блоков цифровых данных технически реализуем и позволяет решить поставленную задачу.

Заявляемый способ может быть реализован, например, на персональных ЭВМ и обеспечивает возможность создания на его основе скоростных программных модулей шифрования и замены дорогостоящей специализированной аппаратуры шифрования персональной ЭВМ, снабженной программной системой скоростного шифрования.

Формула изобретения:

1 Способ шифрования блоков цифровых данных, заключающийся в формировании секретного ключа, разбиении блока данных на N>2 подблоков и поочередном преобразовании подблоков путем осуществления над i-тым подблоком по крайней мере одной операции преобразования, которая зависит от значения j-го подблока, где $j \neq i$, отличающийся тем, что после формирования секретного ключа дополнительно формируют алгоритм шифрования в зависимости от секретного ключа путем формирования по крайней мере одной операции преобразования, которую осуществляют над i-тым подблоком в зависимости от j-го подблока.

2. Способ по п.1, отличающийся тем, что формируют операцию преобразования в виде операции подстановки.

RU 2124814 C1

RU 2124814 C1